Freeware „TCPview“

Netzwerkverbindungen verstehen

Was macht mein Rechner im Netz? Wohin hat er Netzwerkverbindungen aufgebaut? Warum klappt die Verbindung zum Exchangeserver nicht? Um diese und andere Fragen zu beantworten, ist das Programm TCPview ausgesprochen hilfreich.

Unter Windows können Sie sich die Netzwerkverbindungen jederzeit mit dem Kommandozeilentool „netstat“ anzeigen lassen. Dieses Programm ist jedoch sehr spartanisch und lässt sich nur über Kommandozeilenoptionen steuern. Aufgrund der eingeschränkten Möglichkeiten des Kommandozeilenfensters ist die Darstellung nicht besonders übersichtlich.

Kostenloser Download von TCPview

Es gibt jedoch komfortable Werkzeuge, die die graphischen Möglichkeiten der Windowsoberfläche ausnutzen. Eine gute Wahl ist hier die Freeware „TCPview“ von Mark Russinovich von Sysinternals (*www.sysinternals.com*).

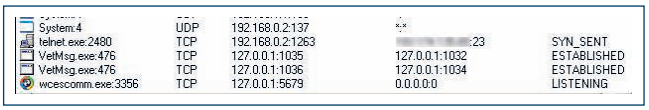
So erkennen Sie, dass eine Firewall die Verbindung verhindert

Jede IP-Verbindung ist in einem von mehreren Zuständen. In der Spalte „State“ wird der Zustand angezeigt.

- „ESTABLISHED“ zeigt eine erfolgreich aufgebaute Verbindung an.
- „SYN_SENT“ zeigt an, dass ein Paket zum Verbindungsaufbau abgeschickt wurde, aber noch keine Antwort vom anderen Rechner angekommen ist. Wird dieser Zustand längere Zeit – also mehr als zehn Sekunden – angezeigt, ist dies meist ein Indiz dafür, dass eine Firewall den Verbindungsaufbau unterbindet.

Auf welche Verbindungen wartet der eigene Rechner eigentlich?

„Listening“ zeigt an, dass der Computer auf einen Verbindungsaufbau wartet. Auf diesen Ports nimmt der Rechner Dienste an.

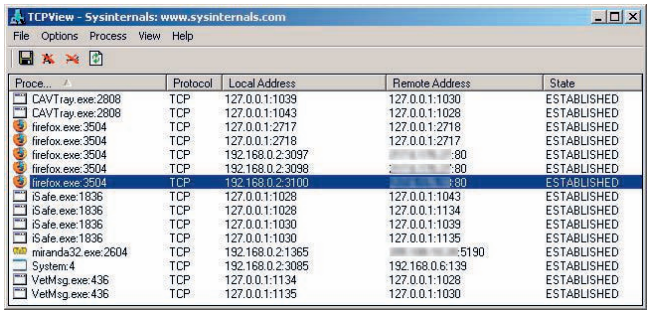


System:4	UDP	192.168.0.2:137	*:*	
telnet.exe:2480	TCP	192.168.0.2:1263	[redacted]:23	SYN_SENT
VetMsg.exe:476	TCP	127.0.0.1:1035	127.0.0.1:1032	ESTABLISHED
VetMsg.exe:476	TCP	127.0.0.1:1036	127.0.0.1:1034	ESTABLISHED
wcescomm.exe:3356	TCP	127.0.0.1:5679	0.0.0.0:0	LISTENING

Zwei auf Verbindungsaufbau wartende Prozesse: Der telnet-Prozess bleibt in einer Firewall hängen, und VetMsg.exe hat zwei lokale Verbindungen aufgebaut.

- Steht vor der Portnummer als IP-Adresse 127.0.0.1, handelt es sich um Dienste, auf die nicht von außen zugegriffen werden kann.
- Wird dort eine „echte“ IP-Adresse angezeigt, wartet der Rechner auf dem zugehörigen Netzwerkinterface auf den Verbindungsaufbau.
- Wird als IP-Adresse 0.0.0.0 angezeigt, wartet der Rechner auf Verbindungsaufbau von überall.

Software kommuniziert ebenfalls per Netzwerkverbindung



Proce...	Protocol	Local Address	Remote Address	State
CAVTray.exe:2808	TCP	127.0.0.1:1039	127.0.0.1:1030	ESTABLISHED
CAVTray.exe:2808	TCP	127.0.0.1:1043	127.0.0.1:1028	ESTABLISHED
firefox.exe:3504	TCP	127.0.0.1:2717	127.0.0.1:2718	ESTABLISHED
firefox.exe:3504	TCP	127.0.0.1:2718	127.0.0.1:2717	ESTABLISHED
firefox.exe:3504	TCP	192.168.0.2:3097	[redacted]:80	ESTABLISHED
firefox.exe:3504	TCP	192.168.0.2:3098	[redacted]:80	ESTABLISHED
firefox.exe:3504	TCP	192.168.0.2:3100	[redacted]:80	ESTABLISHED
ISafe.exe:1836	TCP	127.0.0.1:1028	127.0.0.1:1043	ESTABLISHED
ISafe.exe:1836	TCP	127.0.0.1:1028	127.0.0.1:1134	ESTABLISHED
ISafe.exe:1836	TCP	127.0.0.1:1030	127.0.0.1:1039	ESTABLISHED
ISafe.exe:1836	TCP	127.0.0.1:1030	127.0.0.1:1135	ESTABLISHED
miranda32.exe:2604	TCP	192.168.0.2:1365	[redacted]:5190	ESTABLISHED
System:4	TCP	192.168.0.2:3085	192.168.0.6:139	ESTABLISHED
VetMsg.exe:436	TCP	127.0.0.1:1134	127.0.0.1:1028	ESTABLISHED
VetMsg.exe:436	TCP	127.0.0.1:1135	127.0.0.1:1030	ESTABLISHED

Übersicht über die gerade vom Rechner geöffneten Verbindungen. Der Rechner „redet“ oft mit sich selbst. Externe Verbindungen haben nur firefox.exe und miranda32.exe aufgebaut.

Auch auf einem nicht mit dem Netz verbunden Rechner sieht man eine größere Zahl von Netzwerkverbindungen. Denn die Software kommuniziert über die Netzwerkverbindung zwischen ihren Komponenten.

Eine interessante Aufgabe ist es, erst einmal zu verstehen, was die verschiedenen Prozesse für eine Funktion haben bzw. zu welchem der installierten Softwarepakete sie gehören.

Geben Sie den kompletten Namen des Prozesses einfach in Google ein. Sie werden überrascht sein, wie detailliert viele Prozesse im Internet bereits dokumentiert sind.

Verbindungen und Prozesse beenden

Ein klarer Vorteil des Tools ist die Möglichkeit, über ein Kontextmenü entweder nur die Datenverbindung oder sogar den zugehörigen Prozess zu beenden. Dazu müssen Sie lediglich über die rechte Maustaste das Kontextmenü aufrufen. Dann erhalten Sie die Menüpunkte:

- Process Properties (Eigenschaften des Prozesses anzeigen),
- End Process (Prozess beenden) und
- End Connection (Verbindung beenden).

Gerade über die Prozesseigenschaften hat man einen direkten Zugriff auf das Verzeichnis und die Datei, die zum Prozess gehört.

Details im Web recherchieren

Weiß man nicht, wie ein Programm arbeitet oder was ein Parameter bedeutet, lässt sich auch dies im Internet recherchieren. So können Sie Schritt für Schritt verstehen, wie der eigene Rechner im Netz arbeitet.

Prof. Dr. Rainer W. Gerling

Rainer W. Gerling ist Datenschutzbeauftragter der Max-Planck-Gesellschaft und Honorarprofessor für IT-Sicherheit an der FH München.